Smith form of matrices in companion rings

Vanni Noferini

July 15th, 2025

Me

I am a matrix theorist working at Aalto University (Finland). Interests:

- Matrices over commutative rings
- Random matrix theory
- Graph theory
- Numerical linear algebra
- Numerical analysis

There may be some slight language barrier between communities (?); **please ask me questions** if needed!

The companion matrix of a polynomial

Let $R \neq \{0\}$ be a commutative ring and $g(t) = t^n + \sum_{i=0}^{n-1} g_i t^i \in R[t]$ a monic polynomial. The companion matrix of $g(t)$ is

$$C_g = \begin{bmatrix} -g_{n-1} & \cdots & -g_1 & -g_0 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix} \in R^{n \times n}.$$

(Not explicitly displayed matrix elements are 0.)

The companion matrix of a polynomial

Let $R \neq \{0\}$ be a commutative ring and $g(t) = t^n + \sum_{i=0}^{n-1} g_i t^i \in R[t]$ a monic polynomial. The companion matrix of $g(t)$ is

$$C_g = \begin{bmatrix} -g_{n-1} & \cdots & -g_1 & -g_0 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix} \in R^{n \times n}.$$

(Not explicitly displayed matrix elements are 0.)

Example: $R = \mathbb{Z}$ and $g(t) = t^4 - t^3 + t^2 - t + 1$, then

$$C_g = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Some famous applications

- When $R \subseteq \mathbb{C}$, companion matrices are used to approximate numerically solutions to $g(t) = 0$. Generally, if R is an integral domain (ID), roots of $g(t)$=eigenvalues of C_g (with multiplicities and in the algebraic closure of R).
-

Some famous applications

- When $R \subseteq \mathbb{C}$, companion matrices are used to approximate numerically solutions to $g(t) = 0$. Generally, if R is an integral domain (ID), roots of $g(t)$=eigenvalues of C_g (with multiplicities and in the algebraic closure of R).

  In fact, combined with polynomial approximation, this is the standard approach to numerical rootfinding. One can even exploit the fact that C_g=unitary+rank 1 to compute its eigenvalues much more efficiently than for a generic matrix.

-

Some famous applications

- When $R \subseteq \mathbb{C}$, companion matrices are used to approximate numerically solutions to $g(t) = 0$. Generally, if R is an integral domain (ID), roots of $g(t)$=eigenvalues of C_g (with multiplicities and in the algebraic closure of R).

  In fact, combined with polynomial approximation, this is the standard approach to numerical rootfinding. One can even exploit the fact that C_g=unitary+rank 1 to compute its eigenvalues much more efficiently than for a generic matrix.

- Companion matrices arise naturally when converting a higher order difference or differential equation to first order. For example, Fibonacci numbers can be computed as

$$\begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix} \Rightarrow F_n = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} F_1 \\ F_0 \end{bmatrix}.$$

$(F_{n+2} - F_{n+1} - F_n = 0 \to g(t) = t^2 - t - 1.)$

Companion rings

Given a monic polynomial $g(t)$ with companion matrix C_g, its companion ring is the commutative ring

$$R_g := \{f(C_g) \mid f(t) \in R[t]\} .$$

Well known/easy to prove facts:

-
-
-

Companion rings

Given a monic polynomial $g(t)$ with companion matrix C_g, its companion ring is the commutative ring

$$R_g := \{f(C_g) \mid f(t) \in R[t]\}.$$

Well known/easy to prove facts:

- $R_g \cong R[t]/\langle g(t)\rangle$ by the ring isomorphism

$$f(C_g) \mapsto [f(t)] = \{f(t) + g(t)p(t) | p(t) \in R[t]\}.$$

-
-

Companion rings

Given a monic polynomial $g(t)$ with companion matrix C_g, its companion ring is the commutative ring

$$R_g := \{f(C_g) \mid f(t) \in R[t]\}.$$

Well known/easy to prove facts:

- $R_g \cong R[t]/\langle g(t) \rangle$ by the ring isomorphism

$$f(C_g) \mapsto [f(t)] = \{f(t) + g(t)p(t) | p(t) \in R[t]\}.$$

- When R is an ID, $\det f(C_g) = \prod_{\theta : g(\theta)=0} f(\theta) = \mathrm{Res}(f, g)$.
-

Companion rings

Given a monic polynomial $g(t)$ with companion matrix C_g, its companion ring is the commutative ring

$$R_g := \{f(C_g) \mid f(t) \in R[t]\}.$$

Well known/easy to prove facts:

- $R_g \cong R[t]/\langle g(t)\rangle$ by the ring isomorphism

$$f(C_g) \mapsto [f(t)] = \{f(t) + g(t)p(t) | p(t) \in R[t]\}.$$

- When R is an ID, $\det f(C_g) = \prod_{\theta : g(\theta)=0} f(\theta) = \mathrm{Res}(f, g)$.
- When R is an ID, $g(\theta) = 0$ for $\theta \in \overline{R}$ if and only if $\left(\theta, \begin{bmatrix} \theta^{n-1} \\ \vdots \\ \theta \\ 1 \end{bmatrix}\right)$ is an eigenpair of C_g.

Some famous examples of companion rings

- If $g(t) = t^n$ then C_g is the commutative ring of lower triangular Toepliz matrices. For example when $n = 4$,

$$f(t) \equiv f_3 t^3 + f_2 t^2 + f_1 t + f_0 \mod g(t) \Rightarrow f(C_g) = \begin{bmatrix} f_0 & 0 & 0 & 0 \\ f_1 & f_0 & 0 & 0 \\ f_2 & f_1 & f_0 & 0 \\ f_3 & f_2 & f_1 & f_0 \end{bmatrix}.$$

-

Some famous examples of companion rings

- If $g(t) = t^n$ then C_g is the commutative ring of lower triangular Toepliz matrices. For example when $n = 4$,

$$f(t) \equiv f_3 t^3 + f_2 t^2 + f_1 t + f_0 \mod g(t) \Rightarrow f(C_g) = \begin{bmatrix} f_0 & 0 & 0 & 0 \\ f_1 & f_0 & 0 & 0 \\ f_2 & f_1 & f_0 & 0 \\ f_3 & f_2 & f_1 & f_0 \end{bmatrix}.$$

- If $g(t) = t^n - 1$ then C_g is the commutative ring of circulant matrices. For example when $n = 4$,

$$f(t) \equiv f_3 t^3 + f_2 t^2 + f_1 t + f_0 \mod g(t) \Rightarrow f(C_g) = \begin{bmatrix} f_0 & f_3 & f_2 & f_1 \\ f_1 & f_0 & f_3 & f_2 \\ f_2 & f_1 & f_0 & f_3 \\ f_3 & f_2 & f_1 & f_0 \end{bmatrix}.$$

Less famous examples

- If $g(t) = t^n + 1$ then C_g is the commutative ring of skew-circulant matrices. For example when $n = 4$,

$$f(t) \equiv f_3 t^3 + f_2 t^2 + f_1 t + f_0 \mod g(t) \Rightarrow f(C_g) = \begin{bmatrix} f_0 & f_3 & -f_2 & -f_1 \\ f_1 & f_0 & -f_3 & -f_2 \\ f_2 & f_1 & f_0 & -f_3 \\ f_3 & f_2 & f_1 & f_0 \end{bmatrix}.$$

-

Less famous examples

- If $g(t) = t^n + 1$ then C_g is the commutative ring of skew-circulant matrices. For example when $n = 4$,

$$f(t) \equiv f_3 t^3 + f_2 t^2 + f_1 t + f_0 \mod g(t) \Rightarrow f(C_g) = \begin{bmatrix} f_0 & f_3 & -f_2 & -f_1 \\ f_1 & f_0 & -f_3 & -f_2 \\ f_2 & f_1 & f_0 & -f_3 \\ f_3 & f_2 & f_1 & f_0 \end{bmatrix}.$$

- A nameless example: $g(t) = t^4 - t^3 + t^2 - t + 1$.

$$f(C_g) = \begin{bmatrix} f_0 + f_1 & -f_1 & f_1 - f_3 & -f_1 - f_2 \\ f_1 + f_2 & f_0 - f_2 & f_2 & -f_2 - f_3 \\ f_2 + f_3 & f_1 - f_3 & f_0 + f_3 & -f_3 \\ f_3 & f_2 & f_1 & f_0 \end{bmatrix}.$$

(Note that the bottom row stays “nice", but not the others.)

Elementary divisor domain

An elementary divisor domain (EDD) is an integral domain R over which the following theorem holds.

Theorem (Smith, Kaplansky)

For every $M \in R^{m \times n}$ there exist unimodular $U \in R^{m \times m}$, $V \in R^{n \times n}$ such that $S = UMV$ is diagonal and $S_{ii} \mid S_{i+1,i+1}$ for all $i = 1, \dots, \min(m,n) - 1$. Furthermore (up to units and with the convention $\frac{0}{0} := 0$) it holds

$$S_{ii} = \frac{\gamma_i}{\gamma_{i-1}}$$

where γ_i is the GCD of all minors of size i in M and $\gamma_0 = 1$.

I call S_{ii} the invariant factors of M (including zeros; this may be nonstandard in your community) and γ_i the determinantal divisors of M.

Smith forms of matrices in companion rings

I am interested in studying the Smith form of a matrix $f(C_g)$ with $f(t), g(t) \in R[t]$, $g(t)$ monic, and R EDD.

Smith forms of matrices in companion rings

I am interested in studying the Smith form of a matrix $f(C_g)$ with $f(t), g(t) \in R[t]$, $g(t)$ monic, and R EDD.

I will write $A \sim B$ if there exist unimodular U, V s.t. $A = UBV$ and $A \sim_S B$ if A, B are square and there exists unimodular U s.t. $A = UBU^{-1}$. Clearly $\sim$ is the equivalence relation corresponding to having "the" same Smith form.

Smith forms of matrices in companion rings

I am interested in studying the Smith form of a matrix $f(C_g)$ with $f(t), g(t) \in R[t]$, $g(t)$ monic, and R EDD.

I will write $A \sim B$ if there exist unimodular U, V s.t. $A = UBV$ and $A \sim_S B$ if A, B are square and there exists unimodular U s.t. $A = UBU^{-1}$. Clearly $\sim$ is the equivalence relation corresponding to having "the" same Smith form.

I will now present a selection of results obtained in recent years in collaboration with G. Williams (Essex).

A factorization result

Theorem (VN, Williams)

Let R be an EDD and $f(t), g(t) \in R[t]$ with $g(t)$ monic. Let $z(t) = \gcd(f(t), g(t))$ have degree m, and $f(t) = z(t)F(t)$, $g(t) = z(t)G(t)$. Then

$$f(C_g) \sim F(C_G) \oplus 0_{m \times m}.$$

In particular, the last nonzero determinantal divisor of $f(C_g)$ is $\gamma_r := \mathrm{Res}(F, G)$.

Application to topology

This allowed us to solve a problem in algebraic topology posed in 1975 by Milnor.

Theorem

Let $2 \le r, s, n \in \mathbb{Z}$, with r and s coprime, and define $x := \gcd(r, n), y := \gcd(s, n)$. The homology of the three-dimensional Brieskorn manifold $M = M(r, s, n)$ is

$$H_1(M) \cong \begin{cases} \mathbb{Z}_{r/x}^{y-x} \oplus \mathbb{Z}_{rs/(xy)}^{x-1} \oplus \mathbb{Z}^{(x-1)(y-1)} & \text{if } x \le y; \\ \mathbb{Z}_{s/y}^{x-y} \oplus \mathbb{Z}_{rs/(xy)}^{y-1} \oplus \mathbb{Z}^{(x-1)(y-1)} & \text{if } y \le x. \end{cases}$$

The proof relies on the factorization result, with $R = \mathbb{Z}$, $g(t) = t^n - 1$, and

$$f(t) = \frac{(t^{rs} - 1)(t - 1)}{(t^s - 1)(t^r - 1)} \in \mathbb{Z}[t].$$

Application to group theory

The Gilbert-Howie group $\mathcal{GH}(n, m)$ is the group with generators $x_0, \ldots, x_{n-1}$ and relators $x_0 x_m = x_1$ (subscripts taken $\mod n$).

Application to group theory

The Gilbert-Howie group $\mathcal{GH}(n, m)$ is the group with generators $x_0, \ldots, x_{n-1}$ and relators $x_0 x_m = x_1$ (subscripts taken $\mod n$).

Theorem (VN, Williams)

Fix $m \geq 8$ with $m \equiv 2 \mod 6$. Then there exist at most finitely many integers n, with $n \equiv 0 \mod 6$, such that $\mathcal{GH}(n, m)^{ab} \cong \mathbb{Z}^2$.

Swap theorem

Theorem (VN, Williams)

Let R be an EDD and le $f(t), g(t) \in R[t]$ be monic polynomials of degrees m, n respectively, $m \leq n$. Then,

$$f(C_g) \sim I_{n-m} \oplus g(C_f).$$

Application to group theory

The fractional Fibonacci group $\mathcal{F}^{(k)}(n)$ is the group with generators $x_0, \ldots, x_{n-1}$ and relators $x_0 x_1^k = x_2$ (subscripts taken $\mod n$). These groups generalize Fibonacci groups $\mathcal{F}^{(1)}(n)$ studied by Conway, and are related to the fractional Fibonacci numbers

$$F_0^k = 0, \qquad F_1^k = 1, \qquad F_{j+2}^k = kF_{j+1}^k + F_j^k (j \geq 0).$$

Application to group theory

The fractional Fibonacci group $\mathcal{F}^{(k)}(n)$ is the group with generators $x_0, \ldots, x_{n-1}$ and relators $x_0 x_1^k = x_2$ (subscripts taken $\mod n$). These groups generalize Fibonacci groups $\mathcal{F}^{(1)}(n)$ studied by Conway, and are related to the fractional Fibonacci numbers

$$F_0^k = 0, \qquad F_1^k = 1, \qquad F_{j+2}^k = kF_{j+1}^k + F_j^k (j \geq 0).$$

Theorem (VN, Williams)

Let $n, k \geq 1$. Then $\mathcal{F}^{(k)}(n)^{ab} \cong \mathbb{Z}_\alpha \oplus \mathbb{Z}_\beta$ where

$$\alpha = \gcd(F_n^k, F_{n-1}^k), \qquad \beta = \frac{1}{\alpha}(F_{n+1}^k + F_{n-1}^k - 1 - (-1)^n).$$

Composition theorem

Theorem (VN, Williams)

Let R be an EDD and let $f(t), g(t), h(t) \in R[t]$ where $g(t), h(t)$ are monic. Then,

$$(f \circ h)(C_{g \circ h}) \sim_S f(C_g) \otimes I_{\deg h(t)} \sim_S \underbrace{f(C_g) \oplus \cdots \oplus f(C_g)}_{\deg h(t) \ \textit{times}}.$$

Application to group theory

The generalized Fibonacci group $\mathcal{H}(r, n, s)$ is the group with generators $x_0, \ldots, x_{n-1}$ and relators $x_0 x_1 \ldots x_r = x_{r+1} \ldots x_{r+s-1}$ (subscripts taken mod n).

Application to group theory

The generalized Fibonacci group $\mathcal{H}(r, n, s)$ is the group with generators $x_0, \dots, x_{n-1}$ and relators $x_0 x_1 \dots x_r = x_{r+1} \dots x_{r+s-1}$ (subscripts taken mod n).

Theorem (VN, Williams)

Let $n \geq 2, r \geq 1$ and set $d := \gcd(n, r)$, $N := n/d$. Then,

$$\mathcal{H}(r, n, r)^{ab} \cong \mathbb{Z}_N^{d-1} \oplus \mathbb{Z}^d.$$

The number of non-unit invariant factors

For this theorem, given a PID R and a prime ideal $\langle p \rangle$, we consider the field $\mathbb{F} := R/\langle p \rangle$. For all $f(t) \in R[t]$ we define

$$f_p(t) := [f(t) \mod \langle p \rangle] \in \mathbb{F}[t]$$

as the polynomial such that $f_p(t) \equiv f(t) \mod \langle p \rangle$.

The number of non-unit invariant factors

For this theorem, given a PID R and a prime ideal $\langle p \rangle$, we consider the field $\mathbb{F} := R/\langle p \rangle$. For all $f(t) \in R[t]$ we define

$$f_p(t) := [f(t) \mod \langle p \rangle] \in \mathbb{F}[t]$$

as the polynomial such that $f_p(t) \equiv f(t) \mod \langle p \rangle$.

Example: $R = \mathbb{Z}$, then $\mathbb{F} = \mathbb{F}_p$ is the finite field with p elements. Taking $p = 5$ and $f(t) = t^3 - 11t + 42$, then $f_5(t) = [1]t^3 + [0]t^2 + [4]t + [2]$.

The number of non-unit invariant factors

For this theorem, given a PID R and a prime ideal $\langle p \rangle$, we consider the field $\mathbb{F} := R/\langle p \rangle$. For all $f(t) \in R[t]$ we define

$$f_p(t) := [f(t) \mod \langle p \rangle] \in \mathbb{F}[t]$$

as the polynomial such that $f_p(t) \equiv f(t) \mod \langle p \rangle$.

Example: $R = \mathbb{Z}$, then $\mathbb{F} = \mathbb{F}_p$ is the finite field with p elements. Taking $p = 5$ and $f(t) = t^3 - 11t + 42$, then $f_5(t) = [1]t^3 + [0]t^2 + [4]t + [2]$.

Theorem

Let R be a PID and $f(t), g(t) \in R[t]$ with $g(t)$ monic. Then, the number of non-unit invariant factors of $f(C_g)$ is precisely

$$\max_p \deg \gcd(f_p(t), g_p(t))$$

where the maximum is taken over all primes $p \in R$ dividing γ_r, the last nonzero invariant factors of $f(C_g)$.

Application to group theory

Theorem (VN, Williams)

Let $G_n(h, k; m, q; r, s, \ell)$ be a Cavicchioli-Repovš-Spaggiari group. Then:

- *If G is finite then $\gcd(n, mr) - \gcd(n, m) \leq 3$;*
- *If G is solvable then $\gcd(n, mr) - \gcd(n, m) \leq 4$;*
- *If G is the fundamental group of a closed, connected, orientable three-dimensional manifold M then the Heegaard genus*

$$g(M) \geq \gcd(n, mr) - \gcd(n, m).$$

Second last determinantal divisor

Theorem (VN, Williams)

Let R be an EDD and let $f(t), g(t) \in R[t]$ be coprime, with $g(t)$ monic. Let $q(t) \in R[t]$ be the unique polynomial of degree less than $n = \deg g(t)$ such that $f(t)q(t) \equiv \mathrm{Res}(f,g) \mod g(t)$. Then the second last determinantal divisor of $f(C_g)$ is

$$\gamma_{n-1} = \mathrm{cont}(q(t)).$$

In particular $\gamma_{n-1} = 1$ if and only if $q(t)$ is primitive.

Application

This result has relevance in the study of periodic generalized Neuwirth groups.

Theorem (VN, Williams)

Let $R = \mathbb{Z}$, $n > s \geq 1$, $g(t) = t^n - 1$, $f(t) = b\sum_{i=0}^{s-1} t^i + a\sum_{i=s}^{n-1} t^i$, and define

$$k := \frac{|a(n-s) + sb|}{\gcd(a,b)}.$$

Then the invariant factors of $f(C_g)$ are

$$\gcd(a,b), \underbrace{|a-b|, \ldots, |a-b|}_{n-2 \text{ times}}, k|a-b|.$$